UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A blue Samsung Galaxy Z Fold6 cell phone with a blue and black case currently in the custody of the FBI Portland Division as described in Attachment A

Case No. 3:24-mc-00824

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

A blue Samsung Galaxy Z Fold6 cell phone with a blue and black case currently in the custody of the FBI Portland Division as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1341, 1343, and 1349	Conspiracy to Commit Mail and Wire Fraud

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Craig Robinson, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 4:06 p.m. *(specify reliable electronic means).*

Date: August 9, 2024

Stacie F. Beckerman
Judge's signature

City and state: Portland, Oregon

Hon. Stacie F. Beckerman, United States Magistrate Judge
Printed name and title

ATTACHMENT A

1. The property to be searched is a blue Samsung Galaxy Z Fold6 phone with a blue and black case, which was found on the person of **SINGH** at the time of the traffic stop that occurred on July 12, 2024, hereinafter "Device 1." Device 1 is currently in the custody of the FBI Portland Division located at 9109 NE Cascades Blvd., Portland, Oregon and identified and stored under FBI Case Number 196D-PD-3929089, Evidence Item 1B20.

2. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on Device 1 (the Device), as described in Attachment A, that relate to violations of Title 18, United States Code, Sections 1341, 1343, and 1349, to-wit: engaging in a conspiracy to commit mail and wire fraud and involve **Navjot SINGH,** including:

a. All records, documents, or materials, including correspondence, pertaining to the commission of, or conspiracy to commit, mail fraud and wire fraud, as those terms are defined in 18 U.S.C. §§ 1341, 1343, and 1349;

b. lists of victims and related identifying information;

c. any information related to co-conspirators and associates involved in the above violations (including names, addresses, phone numbers, or any other identifying information);

d. any information recording **SINGH's** schedule or travel from **January 1, 2024,** to the present; and,

e. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or

stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF CRAIG ROBINSON

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT FOR PHONE

I, Craig Robinson, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for approximately one year. I am currently assigned to the FBI Portland Field Office's Salem Resident Agency squad. As a federal law enforcement officer, I am authorized to investigate and make arrests for violations of federal law, and to apply for federal search warrants. I completed a 21-week course of instruction at the FBI Academy in Quantico, Virginia, which consisted of specialized training in investigating a range of criminal violations. I acquired knowledge and information about crimes from many sources, including formal and informal training, other law enforcement officers and investigators, persons who I have interviewed, and my participation in numerous investigations. I have investigated matters involving fraud and online scams, particularly as they relate to violations of Title 18 of the United States Code, Sections 1341 and 1343 involving wire and mail fraud.

2. I submit this affidavit in support of an application for a search warrant authorizing the search of Navjot **SINGH's** cellular telephone (also referred to as **Device 1**) as described in Attachment A, for evidence, contraband, fruits, and instrumentalities, as described in Attachment B, of violations of Title 18, United States Code, Sections 1341, 1343, and 1349, which prohibit persons from conspiring to devise or intending to devise any scheme or artifice to defraud by means of mail or wire communications (the Target Offenses).

///

Identification of Device to be Examined

3. **Device 1** is a blue Samsung Galaxy Z Fold6 phone with a blue and black case (hereinafter "**Device 1**"), which was found on the person of Navjot **SINGH** (hereinafter **SINGH**) at the time of his traffic stop and arrest that occurred on July 12, 2024. **Device 1** is currently in the custody of the FBI Portland Division located at 9109 NE Cascades Blvd., Portland, Oregon. **Device 1** is further identified and stored under FBI Case Number 196D-PD-3929089, Evidence Item 1B20, and described in Attachment A.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The statements contained in this affidavit are based upon the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

Applicable Law

5. Title 18, United States Code, Section 1341, prohibits a person, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, for the purpose of executing such scheme or artifice or attempting so to do, placing in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or depositing or causing to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing,

or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing.

6. Title 18, United States Code, Section 1343, prohibits a person, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

7. Title 18, United States Code, Section 1349, prohibits a person from attempting to conspiring to commit a violation of Title 18, United States Code, Sections 1341 and 1343.

Statement of Probable Cause

8. On July 3, 2024, Adult Victim 1, born in 1947, and Adult Victim 2, also born in 1947, a husband and wife living in West Linn, Oregon, contacted the FBI Portland Division to report that they believed they were victims of fraud being committed by individuals impersonating FBI Agents. At the time of reporting, Adult Victims 1 and 2 had lost approximately $279,475 as a result of the fraud scheme.

9. Adult Victim 1 reported this all started on June 3, 2024, when he was on his computer and his screen went black and a message popped up instructing him to call the number on the screen. Adult Victim was reluctant and did not call this number. However, about a month or so before this incident, Adult Victim 1 had received an electronic message from someone claiming to be from Microsoft which instructed him to check his credit card statements for any

unusual charges. This message also provided a number for Adult Victim 1 to call if he ever had any issues arise with his computer. Adult Victim 1 called this purported "Microsoft" number, which he believed was a Microsoft helpdesk number, and he was informed that his computer system would be fixed, but that they first had to transfer him to a Special Agent with the FBI who was investigating the matter. Adult Victim 1 was then transferred to an individual claiming to be an FBI Special Agent named Jon Stryker (Stryker).

10. According to Adult Victim 1, Stryker told Adult Victim 1 that he and his wife "were in danger" and they needed to be in constant contact with him to help ensure their safety. Adult Victim 1 took this to mean they were in some sort of physical danger. Stryker also informed the victims that they needed to download a program to help ensure the safety of their computer, which they did. Adult Victim 1 reported that after doing this his computer was taken over remotely and a four-page document with the heading "National Cyber Investigative Joint Task Force" popped up on the screen. The document stated that this was all part of a confidential FBI investigation and not to tell anyone about it. The document referenced the U.S. Code and several U.S. Acts that allegedly made it illegal for Adult Victims 1 and 2 to tell anyone about what was going on. The document also referenced a recent incident that supposedly happened where the FBI's computers and servers were hacked and a FBI agent died during a sting operation associated with "Lockbit." The document stressed that Adult Victims 1 and 2 had to comply with the document or face legal consequences.

11. Over the next few weeks, Adult Victims 1 and 2 maintained regular communications with Stryker via phone and text messages in which Stryker continued to inform them that they remained in danger. During this time, Stryker gave the Victims instructions to

share their personal information and bank statements with him, which they did. Stryker told Adult Victims 1 and 2 that he had drones that were keeping an eye on their home and he was making sure they were safe. During one conversation Stryker made a comment to them about some work he knew they were having done on their fence in the backyard. Adult Victims 1 and 2 believed they were being watched by Stryker.

12. On June 17, 2024, Adult Victim 2's computer, a separate computer in the household, showed the same type of document as the one that appeared on Adult Victim 1's computer, as mentioned above, and her computer was also remotely taken over. The document listed one of their Social Security numbers and stated that the number had been used to buy servers that were used in connection with a cyber-attack against the FBI. At this time the Victims were also informed that their financial assets were at risk and that hostile actors could seize their assets and that their assets could also be frozen by the IRS. Adult Victims 1 and 2 were instructed to secure their assets in the FBI-Secure Vault Service for safekeeping. Stryker informed the Victims that gold was the most secure asset and then gave them specific instructions to purchase gold bars and package them in a sealed carboard box. Stryker told the Victims he would schedule a time for an "Agent" to come and collect the gold from them and it would be transported to the FBI-Secure Vault.

13. On June 17, 2024, Adult Victim 2 made a wire transfer to purchase $279,475 in gold bars from Prefinery USA Inc. On June 18, 2024, the wire transfer processed through Adult Victim 2's bank account. On June 22, 2024, the gold bars then were shipped to the Portland Gold Exchange store. Adult Victim 2 informed Stryker that the gold arrived and Stryker scheduled a pickup for the gold around 12:00 p.m. to occur at Adult Victim 1 and 2's residence

in West Linn, Oregon. On June 22, 2024, the day of the pickup, Stryker contracted the Adult Victims and told them that a FBI Agent in a white Jeep Wrangler was circling their neighborhood. At approximately 3:51 p.m., on the day of the pickup, Stryker instructed Adult Victim 2 to go outside with the gold bars and place them, through the rear window, into the back seat of the Jeep Wrangler. Adult Victim 2 observed the driver and described him as a very tan male, with dark half inch long hair, a very short stubble beard, and having a long oval shaped face. Adult Victim 2 did as she was instructed and placed a box containing the gold bars in the back seat of the Jeep, which then drove off.

14. After contacting the FBI Portland Division on July 3, 2024, Adult Victims 1 and 2 informed Agents that Stryker had reached out to them again and this time they were instructed to purchase an additional $193,000 in gold bars and that he would schedule another pickup with an "Agent." Agents and officers from the West Linn Police Department then prepared a controlled pickup operation that took place on July 12, 2024. Agents instructed Adult Victims 1 and 2 to notify Stryker that they had purchased approximately $193,000 in gold bars that could be picked up on July 12, 2024.

15. On July 12, 2024, at approximately 1:55 p.m., Agents and officers observed a black BMW X1 SUV (target vehicle) driving along the streets near Adult Victims 1 and 2's house. Officers and Agents observed the target vehicle stop in front of Adult Victims 1 and 2's residence. Adult Victim 2 walked to the target vehicle with a decoy package while she was on the phone with Stryker. Adult Victim 2 then placed the decoy package in the back seat of the target vehicle through the rear window and the vehicle drove off.

///

16. Officers and Agents observed the target vehicle depart from Adult Victim 1 and 2's residence at a fast rate of speed and turn south. Shortly thereafter a marked patrol unit with West Linn Police Department conducted a traffic stop on the target vehicle. The driver in the target vehicle was identified as **SINGH**. **SINGH** was holding **Device 1** when he was contacted by officers. The officers seized **Device 1** and later handed it over to me. I subsequently placed **Device 1** into evidence at the FBI Office in Portland, Oregon. Inside the vehicle Detectives and Agents observed the decoy package sitting on the rear seat.

17. **SINGH** provided verbal consent to search the target vehicle. During the search, Agents located a booking ticket for Delta Airlines, dated July 12, 2024, in **SINGH**'s name which showed that he had flown into Portland, Oregon that day from Atlanta, Georgia. Agents also observed a black backpack that was identified as belonging to **SINGH** that contained a few items of clothes and toiletries, which I would estimate was enough for one to two days of travel.

18. During the traffic stop, **SINGH** informed Agents and officers that he lived in South Carolina. When asked what he was doing in Oregon, **SINGH** initially told Agents and Detectives that he arrived in Portland about two days ago. **SINGH** later recanted and stated that he arrived in Portland yesterday. When asked what brought him to Portland, **SINGH** initially stated that he was in Portland for construction work and that he received a WhatsApp call from an unknown person with the number 470-751-7063 asking him if he would pick up a package and deliver it to California. When asked what the name of the construction company was that he was working for, **SINGH** stated it was Gomez Construction. **SINGH** later stated that he was unemployed and had not been working for seven months due to a car accident where he injured his back. When asked why he flew out of Atlanta instead of Columbia or Charlotte airports,

SINGH stated that he was staying with his girlfriend. **SINGH** then stated that he and his girlfriend were together for four months and they broke up two months ago, and that he was actually staying at his home in Columbia the past 6 months. **SINGH** then stated his friend drove him from Columbia to Atlanta to fly to Portland. **SINGH** told Agents and officers that the unknown caller purchased his airline ticket from Atlanta to Portland and that he purchased the rental vehicle he was stopped in, a black BMX X1 SUV. **SINGH** also mentioned that he had no family here in the United States, that they all lived in India. Later, while at the West Linn Police Department, **SINGH** invoked his right to an attorney and Agents ceased asking him questions.

19. After **SINGH** was arrested and while he was in custody the Victims received repeated "urgent" messages from Stryker asking them to contact him. The Victims eventually blocked Stryker's number.

20. After **SINGH** was arrested we learned through travel records that he had flown from Charleston, South Carolina into the Portland, Oregon airport on June 22, 2024, the day the Victims handed over the first package, and on June 24, 2024, he flew from Portland back to Charleston, South Carolina.

21. I know from this investigation that **SINGH** has admitted to using his cellular telephone (**Device 1**) to communicate with at least one other member of the conspiracy in which he was instructed to pick up a package at the Victim's residence and deliver it to California and as a result of these communications he then picked up a package, which was supposed to contain gold, on the day he was arrested. Accordingly, I believe there is probable cause to believe there are communications and other evidence of the Target Offenses, as outlined in Attachment B, within **Device 1**.

Search and Seizure of Digital Data

22. This application seeks permission to search for particular items, described in Attachment B, in whatever form those items may be found. One form in which that evidence will likely be found is as data stored on a digital device, including a cell phone. Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

23. Specifically, this application seeks permission to search for, seize, and examine:

a. All records, documents, or materials, including correspondence, pertaining to the commission of, or conspiracy to commit mail fraud and wire fraud, as those terms are defined in 18 U.S.C. §§ 1341, 1343, 1349;

b. Evidence of Internet usage for the commission of, or conspiracy to commit, mail fraud and wire fraud as defined in 18 U.S.C. §§ 1341, 1343, 1349, including dates and times of usage; IP addresses; and screennames, usernames, and passwords used to access the Internet or any accounts via the Internet;

c. Communications, including emails, chats, bulletin board posts, and comments. relating to the commission of, or conspiracy to commit, mail fraud and wire fraud; and

d. "Records," "items," "documents," and "materials" include all of the foregoing items in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

///

24. Based on my training and experience and the knowledge obtained from other law enforcement officers, I know criminals involved in fraud crimes often try to conceal their methods of communication and their communication devices from law enforcement in order to use these devices to conduct their criminal activities without being caught. One such method of concealing communication methods and devices is to use multiple different communication devices, often changing which one is used. Based on my training and experience and the circumstances described herein, I believe **SINGH** used **Device 1** to communicate and conduct illegal activity related to the Target Offenses and that specific evidence, fruits, or instrumentalities of such illegal fraudulent activity will be found on the Phone.

25. In addition to the facts listed previously, I believe the facts and circumstances establish probable cause that the electronically stored information described in Attachment B is located on **Device 1**, as described in Attachment A.

26. The Phone is currently in the lawful possession of the FBI Portland Division located at 9109 NE Cascades Blvd, Portland, Oregon. **Device 1** was seized by FBI Special Agents during **SINGH**'s traffic stop followed by his arrest. In my training and experience, I know that the Phone has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as when the Phone first came into the possession of the FBI.

27. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A

wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet, including the use of apps. Wireless telephones may also include a global positioning system ("GPS") technology for determining the location of the device.

28. Based on my training, experience, and research, I know that the Phone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

29. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant but also forensic evidence that establishes how the Phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Phone because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with

forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person "deletes" a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Phone may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Data on the Phone can provide evidence of a file that was once on the Phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals,

including SD cards or other flash media, and the times the Phones were in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

f. A person with appropriate familiarity with how the Phones work may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Phones is evidence may depend on other information stored on the Phones and the application of knowledge about how Phones function. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how the Phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the Phone.

30. I know that when an individual uses a wireless telephone to commit a crime such as to communicate about or arrange mail or wire fraud, the phone will generally serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime.

From my training and experience, I believe that a phone used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phone consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

32. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

33. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file

///

system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

34. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phones, absent further authorization from the Court.

35. If the Phone contains evidence, fruits, contraband, or is an instrumentality of the crime, the government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

36. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

37. *Manner of execution*. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

///

///

Conclusion

38. Based on the foregoing information, I respectfully submit that there is probable cause to believe that the phone described in Attachment A (**Device 1**) contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1341, 1343, and 1349, as set forth herein and in Attachment B. I therefore respectfully request that the Court issue a warrant authorizing a search of the cell phone (**Device 1**) described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

39. This affidavit, the accompanying application, and the requested search warrant were reviewed by Assistant United States Attorney (AUSA) Scott Kerin prior to being submitted to the Court. AUSA Kerin informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone pursuant to Fed. R. Crim. P. 4.1
CRAIG ROBINSON
Special Agent
Federal Bureau of Investigation

Sworn via telephone pursuant to Fed. R. Crim. P. 4.1 at 4:06 p.m. on August 9, 2024.

Stacie F. Beckerman
HONORABLE STACIE F. BECKERMAN
United States Magistrate Judge